51. (New) A method of encrypting a message using the public key generated by the business method of claim 50.

52. (New) A method of decrypting a message using the public key and the private key generated by the business method of claim 50.

53. (New) A method of signing a message using the public key and the private key generated by the business method of claim 50.

54. (New) A method of verifying a signature using the public key generated by the business method of claim 50.

55. (New) A method of key exchange using the public key and the private key generated by the method of claim 50.

56. (New) A method of performing a Diffie-Hellman key exchange or a related scheme using *p*, *q*, and *B* as generated by the business method of claim 49.

REMARKS

Upon entry of this Supplemental Preliminary Amendment, claims 1-24 have been canceled, claims 25-56 have been added, and claims 25-56 are pending in the application. Claims 25, 33, 41, and 49 are in independent form.

Appendix 1 shows the changes made to each paragraph replaced by this Amendment relative to the previous version of the paragraph in the Substitute Specification. The Applicants respectfully request examination of this case and early issuance of a Notice of Allowance.

AUTHORIZATION

The Assistant Commissioner is hereby authorized to charge any additional fees which may be required for the timely consideration of this amendment under 37 C.F.R. §§ 1.16 and 1.17, or credit any overpayment to Deposit Account No. 13-4500, Order No. 0225-4188.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Kenneth P. Waszkiewicz.

Kenneth P. Waszkiewicz
Registration No. 45,724

SENDER'S ADDRESS:

MORGAN & FINNEGAN, L.L.P.
345 Park Avenue
New York, NY 10154-0053

202-857-7887 - phone
202-857-7929 - fax

Dated: May 11, 2001

APPENDIX 1

MARKED-UP REPLACEMENT PARAGRAPHS IN THE SPECIFICATION

This appendix shows the changes made to each paragraph replaced by this Amendment relative to the previous version of the paragraph. All additions are shown underlined (e.g., the) and all deletions are shown in brackets (e.g., [the]).

REPLACE the paragraph on page 3, lines 13-29 of the Substitute Specification with the following:

The method of the invention determines a public key having a reduced length and a [factor] number p, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6). The method includes the step of selecting a number p and a prime number q that is a divisor of $p^2 - p + 1$. Then the method selects an element g of order q in GF(p^6), where g and its conjugates can be represented by B, where $F_g(X) = X - BX^2 + B^p X - 1$ and the roots of $F_g(X)$ are [g, g^{p-1}, and g^{-p}] g, g^{p-1}, and g^{-p}. Then the method represents the powers of g using their trace over the field [$GF(p^2)$] GF(p^2). The method then selects a private key. The method then computes a public key as a function of g and the private key. The public key can be used to encrypt a message and the public and private key can be used to decrypt the message. The public and private key can be used for signing a message and the public key can be used for verifying the signature. A [Diffie Hellman] Diffie-Hellman key exchange or other related scheme can be conducted using the public key generated by the method. The resulting invention reduces the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, and reduces the computational effort required to encrypt/decrypt and to generate/verify digital signatures.

DELETE the current Abstract of the Disclosure and INSERT the following:

Efficient and Compact Subgroup Trace Representation ("XTR")

Abstract of the Disclosure

The invention is a method, system, computer program, computer program article of manufacture, and business method for providing improvements in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and [the] to generate/verify digital signatures. The method of the invention determines a public key having a reduced length and a [factor] number p, using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6).